Содержание

1 Характеристики международных стандартов ИБ

Классификация стандартов:
- Национальные стандарты(ГОСТ и ГОСТ Р)
- Стандарты предприятий и организаций (ТУ, СТП, СТО)
- Международные стандарты(ISO, МЭК)

Виды стандартов:

- Стандарты основополагающие
- Стандарты на продукцию, услуги
- Стандарты на процессы
- Стандарты на методы контроля, испытаний, измерений и анализа

Международные и отечественные стандарты предполагают:

1. Определение целей ИБ КИС
2. Создание эффективной системы управления ИБ
3. Расчет совокупности детализированных качественных и количественных показателей для оценки соответствия ИБ поставленным целям
4. Применения инструментария обеспечения ИБ и оценки ее текущего состояния
5. Использования методик управления безопасностью

Наиболее распространенными управленческими стандартами являются стандарты разработанные Британским университетом стандартов.

1.1 Стандарт ISO/IEC 17799-2005(Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению безопасностью.)

Представляет собой набор практических рекомендаций по построению комплексной корпоративной системы управления ИБ.

ИБ рассматривается как процесс защиты информационных активов организации от различного рода угроз, которые достигаются путем реализации определенных механизмов контроля.

Требования к системе безопасности определяется по результатам предварительного проведенным анализам риска и требований нормативных и законодательных актов, а также путем анализа специфических потребностей бизнеса.

Механизмы контроля выбираются таким образом, чтобы минимизировать идентифицированные риски. Основное содержание стандарта составляет каталог рекомендуемых механизмов контроля безопасности. Механизмы сгруппированы по тематическим разделам:

- Политика безопасности
- Организация ИБ
- Управление Активами
- Безопасность людских ресурсов
- Физическая безопасность и безопасность окружающей среды
- Управление телекоммуникациями
- Управление доступом
- Приобретение, разработка, внедрение ИС
- Управление инцидентами в сфере ИБ
- Управление непрерывностью бизнеса
- Соответствие

Для каждого механизма контроля приведены его определения, руководства по его реализации, представлена дополнительная документация.

1.2 ISO 27001-2005(Информационные технологии. Методы обеспечения безопасности. Системы управления ИБ. Требования)

— Представляет собой расширенный ISO 17799, устанавливающего требования по созданию, эксплуатации, мониторингу, анализу, поддержке и совершенствованию корпоративных систем ИБ.

Организация СУИБ осуществляется по системе PDCA(планирование, реализация, анализ, корректировка).

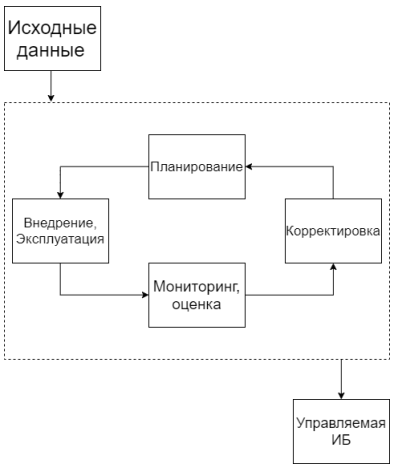

Рис.1 Схема осуществления системы СУИБ

1.3 BS 7799-3:2006 (Система управления систем ИБ — Руководство по управлению рисками по ИБ)

— набор руководств и рекомендаций, которые направлены на удовлетворение требований стандарта 27001-2005 в части управления рисками. Стандарт не содержит требований по использованию какой-либо методики управления рисками. Предъявляет 4 требования:

- Возможность определения риска
- Возможность идентификации приемлемых уровней риска
- Возможность проведения идентификации оценки риска
- Покрытие всех аспектов системы ИБ

Стратегии управления ИБ:

1. Уменьшение риска
2. Осознанное принятие риска
3. Передача риска
4. Избежание риска

Деятельность, которая связанна с реализацией управления рисками, должна сопровождать с планом реализации рисков. Непрерывный процесс реализации рисков в организации должен контролироваться специалистом либо группой специалистов.

Германский стандарт BSI:

- Общая методика ИБ
- Описание компонентов ИТ
- Описание основных компонентов режима ИБ
- Характеристики объемов информации
- Характеристики основных информационных объектов компании
- Характеристики компьютерных сетей на основе различных технологий
- Характеристики активного и пассивного оборудования
- Подробные каталоги угроз безопасности и мер контроля(более 600 наименований в каждом каталоге)

Вопросы защиты приведенных активов рассматриваются по сценарию:

- Общее описание информационных активов компании
- Возможные угрозы безопасности
- возможные меры и средства контроля защиты

1.4 Стандарт ISO/IEC 15408-1999(Общие критерии)

— обобщил содержание и опыт использование "Оранжевой книги развил европейские и канадские критерии и воплотил в реальные структуры концепцию типовых профилей защиты федеральных критериев США. Проведена классификация широкого набора требований безопасности ИТ. Определены структуры, их группирование и принципы устройства. Полнота требований безопасности и их систематизация, также являются гибкими для дальнейшего развития.

В соответствие с ним ИБ рассматривается как единство конфиденциальности и целостности информации. Выдвигают средствам защиты критерии защиты информации. Регламентируют все стадии разработки квалификационного анализа и эксплуатации продуктов информационных технологий. Требования Общих критериев можно использовать в качестве справочника по безопасности ИТ.

1.5 Стандарты ИБ для Беспроводных сетей и сети Интернет

— В основы этого вида стандарта положены разработки рабочей группы 802.11 комитета IEE. В 1997 году был принят стандарт 802.11, полоса частот 2.4 ГГц, скорость – 1-2 Мбит/сек. Является базовым и определяет протоколы, которые необходимы для организации беспроводных локальных сетей. Главный из них протокол управления доступом в среде MAC и протокол PHY(Передача посредством радиоволн и ИК).

Основой составляет сотовая архитектура. Может состоять как из 1, так и нескольких ячеек(сот). Каждая из них управляет базовой станцией(точкой доступа – AP). AP образует базовую зону обслуживания(BSS). Точки доступа взаимодействую через распределительную систему(DS). Вся инфраструктура в совокупности с AP и DS образует расширенную зону обслуживания(ESS). Данным стандартом также предусмотрен одно-сотовый вариант сети. Для обеспечения перехода мобильных рабочих станций из зоны действия AP к другой точке доступа в много-сотовых системах предусмотрены специальные процедуры сканирования(активного и пассивного прослушивание эфира) и присоединения. Строгих спецификаций по реализации роуминга данный стандарт не предусматривает.

1.6 Гост Р 53114-2008 защита информации. Обеспечение ИБ в организации. Основные термины и определения.

Безопасность информации(данных) — состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Информационная инфраструктура — совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

Критический объект(ИБ) — объект или процесс нарушения непрерывности функционирования, которого может нанести значительный ущерб.

Оценка риска ИБ(организации) — общий процесс идентификации, анализа и определения приемлемости уровня риска ИБ организации.

Угроза ИБ(организации) — совокупность факторов и условий, создающих опасность нарушения ИБ организации, вызывающей или способной вызвать негативные последствия, ущерб или вред организации.

2 Национальный стандарт ГОСТ Р ИСО/МЭК 27001-2006. ИТ.(Практика)

ГОСТ Р ИСО/МЭК 27001-2006.(Информационные Технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности.)

Конфиденциальность — свойство информации быть недоступной и закрытой для неавторизованного субъекта, логического объекта или процесса.

ИБ — свойство информации сохранять целостность, конфиденциальность и доступность.

СМИБ(система менеджмента ИБ) — часть общей системы менеджмента, основанная на использовании методов оценки бизнес рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения ИБ.

1 — Что должна включать в себя документация СМИБ?

Положения политики СМИБ и целей СМИБ, Область функционирования СМИБ, процедуры и меры управления, поддерживающей СМИБ, описание методологии СМИБ, отчет по оценке рисков, план обработки рисков, документированные процедуры, необходимые организации для обеспечения эффективного планирования, внедрения процессов в области ИБ и управления этими процессами, учетные записи, положения о применимости

2 — Что необходимо сделать для предоставления свидетельств, соответствия требований и результативности СМИБ? Необходимо вести и поддерживать в рабочем состоянии учетные записи, записи должны быть четкими, легкоидентифицируемыми и восстанавливаемыми.

Организация должна выполнить следующие требования:

- Разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ
- реализовать план обработки рисков для достижения намеченных целей управления, включающие в себя вопросы функционирования, а также распределения функций и обязанностей.
- внедрить меры управления для достижения целей управления
- определить способ измерения результативности выбранных мер управления или их групп
- реализовать программу по обучению и повышению квалификации сотрудников
- управлять работой СМИБ
- внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирования на инциденты, связанные с ИБ

3 ГОСТ Р ИСО/МЕК 27001(Практика)

1 — Какие аудиты должна проводить организация в соответствие с утвержденным графиком по СМИБ?

Организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СМИБ, позволяющие установить, что цели управления, меры управления, процессы и процедуры СМИБ:

a) соответствуют требованиям настоящего стандарта и соответствующим законам или нормативным документам;

b) соответствуют установленным требованиям ИБ;

c) результативно внедряются и поддерживаются;

d) функционируют должным образом

2 — Какую информацию должны включать входные данные для анализа СМИБ со стороны руководства?

Входные данные для анализа СМИБ со стороны руководства должны включать в себя следующую информацию:

a) результаты предыдущих аудитов и анализа СМИБ;

b) результаты взаимодействия с заинтересованными сторонами;

c) методы, средства или процедуры, которые могут быть использованы в организации для совершенствования функционирования и повышения результативности СМИБ;

d) правовое обоснование предупреждающих и корректирующих действий;

e) уязвимости или угрозы, которые не были адекватно учтены в процессе предыдущей оценки рисков;

f) результаты количественной оценки результативности СМИБ;

g) последующие действия, вытекающие из предыдущего анализа со стороны руководства;

h) любые изменения, которые могли бы повлиять на СМИБ;

i) рекомендации по улучшению.

3 — Какие требования должна устанавливать документированная информация корректирующая действия

Документированная процедура корректирующего действия должна устанавливать требования по:

a) выявлению несоответствий;

b) определению причин несоответствий;

c) оцениванию необходимости действий во избежание повторения несоответствий;

d) определению и реализации необходимых корректирующих действий;

e) ведению записей результатов предпринятых действий

f) анализу предпринятого корректирующего действия.

Аудит ИБ — системный процесс получения объективных, качественных и количественных оценок о текущем состоянии ИБ АС в соответствие с определенными критериями и показателями безопасности

4 Отечественные стандарты ИБ

Характеристика отечественных стандартов ИБ:

- Руководящие документы ФСТЭК РФ
- ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий"("Общие критерии") — введен в действие с 01 января 2004 года, в перспективе "Общие критерии"должны заменить руководящие документы ФСТЭК РФ во всех сертификации средств защиты информации. В настоящее время оба поколения стандартов используются одновременно. Применяется исключительно при проведении сертификации продуктов не предназначенных для обработки информации, которые составляют признаки Гос. тайны.

4.1 Руководящие документы ФСТЭК РФ

С 1992 до 1999 годы ФСТЭК РФ разработала пакет руководящих документов, которые посвящены вопросам защиты информации в автоматизированных системах(АС). Среди них наиболее важными являются:

- Защита от НСД. Термины и определения.
- Концепции защиты СВТ и АС от НСД к информации.
- АС. Защита от НСД к информации. Классификация АС и требования по защите информации.
- СВТ. Защита от НСД к информации. Показатель защищенности от НСД к информации.
- СВТ. Межсетевые экраны. Защита от НСД. Показатели защищенности от НСД к информации.
- Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей.

4.1.1 Основные положения концепции защиты СВТ и АС от НСД к информации.

НСД — доступ к информации, который нарушает установленные правила нарушения доступа с использованием штатных средств, предоставляемыми СВТ или АС.

`Выделяют 2 направления защиты от НСД:`

1. Связанное с СВТ
2. Связанное с АС

СВТ — представляет собой элементы из которых состоит АС. Для СВТ контролируется выполнение исключительно тех функций защиты, для реализации которых они предназначены, в отличие от АС.

`Существует следующие способы НСД:`

- Непосредственное обращение к объектам доступа.
- Создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты.
- Модификация средств защиты, позволяющая осуществить НСД(программные закладки).
- Внедрение в технические средства(СВТ или АС) программных или технических механизмов, которые нарушают предполагаемую структуру и функции СВТ или АС и позволяют осуществить НСД.(Загрузка ПК в обход штатной ОС)

`Принципы защиты от НСД СВТ и АС:`

- Основывается на положениях и требованиях, соответствующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.
- Для СВТ — Использование комплекса программно-технических средств.
- Для АС — Использование комплекса программно-технических средств и организационные меры.
- Должна обеспечиваться на всех этапах обработки информации.(В том числе при проведении ремонтных, регламентных работ)
- Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС(надежность, быстродействие, возможность изменения конфигурации АС).

- Оценка эффективности средств защиты, которая осуществляется по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, должна соответствовать требуемому уровню.
- Защита АС и СВТ должна предусматривать контроль эффективности средств защиты от любых видов НСД.

В качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС или СВТ.

`Уровни доступа нарушителя:`

1. 1 уровень – возможность ведения диалога(запуск программ из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации)
2. 2 уровень – возможность создания и запуска собственных программ с новыми функциями по обработке информации.
3. 3 уровень – возможность управления функционирования АС(воздействия на базовое программное обеспечение системы, а также на состав и конфигурацию ее оборудования).
4. 4 уровень – весь объем возможности лиц, осуществляющих проектирование, реализацию, ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Оценку технических средств защиты от НСД предлагается производить по следующих характеристикам:

- По степени полноты и качеству охвата правил разграничения доступа, реализована система разграничения доступа(СРД).(оценивается четкость и непротиворечивость правил доступа. Надежность идентификации правил доступа)
- Состав и качество обеспечивающих средств для СРД(Оценка учитывает: средства идентификации и опознавания субъектов, и порядок их использования. Полноту учета действий субъектов. Способы поддержания привязки субъекта к его процессу)
- Гарантий правильности функционирования СРД и обеспечивающих ее средств.

4.1.2 СВТ. Защита от НСД к информации. Показатель защищенности от НСД к информации

Документ устанавливает классификацию по уровню защищенности от НСД к информации на базе перечня показателя защищенности и совокупности, описывающих их требований.

СВТ рассматривается в качестве совокупности программных и технических элементов АС, которые функционируют самостоятельно или в составе других систем.

Устанавливаются 7 классов защищенности к СВТ от НСД, которые разбиваются на 4 группы:

- `I группа` — 7 класс — СВТ представленные к оценке, но не удовлетворяющие требованиям более высоким классам.
- `II группа` — 6-5 класс — Дискреционная защита.
- `III группа` — 4, 3, 2 класс — Мандатная защита.
- `IV группа` — 1 класс — Верифицированная защита.

С уменьшением номера класса требования ужесточаются. Каждый класс характеризуется фиксированным набором показателей защищенности. Классы иерархически упорядочены. Каждый последующий класс содержит требования предыдущих.

В общем случае требования предъявляются к 21 показателю защищенности. Оценка класса защищенности СВТ осуществляется путем проведения сертификационных испытаний.

4.1.3 АС. Защита от НСД к информации. Классификация АС и требования по защите информации.

Документ устанавливает классификацию АС, подлежащих защите от НСД к информации и задает требования по защите информации в АС различных классов.

`Классификация АС включает следующие этапы:`

1. Разработка и анализ исходных данных.
2. Выявление основных признаков АС, необходимых для классификации.

3. Сравнение выявленных признаков с классифицируемыми.

4. Присвоение АС соответствующего класса защиты информации от НСД.

`Исходные данные для классификации АС являются:`

- Перечень защищаемых информационных ресурсов АС и уровень их конфиденциальности.
- Перечень лиц, имеющих доступ к штатным средствам АС с указанием их уровня полномочий.
- Матрицы доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС.
- Режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалиста по защите информации.

Устанавливается 9 классов защищенности АС от НСД к информации:

- `III группа` — 3Б, 3А классы — эти классы соответствуют АС, в которых работает 1 пользователь, который допущен ко всей информации в АС, размещенной на носителях одного уровня конфиденциальности.
- `II группа` — 2Б, 2А — эти классы соответствуют АС, в которых пользователи имеют одинаковые права доступа ко всей информации в АС, обрабатываемой или хранимой на носителях различного уровня конфиденциальности.
- `I группа` — 1Д, 1Г, 1В, 1Б, 1А — Одновременно обрабатывается или хранится информация разных уровней конфиденциальности. Не все пользователи имеют доступ ко всей информации АС.

Для каждого из классов фиксируется набор требований к следующим подсистемам:

- Подсистема управления доступом.
- Подсистема регистрации и учета.
- Подсистема криптографической защиты.
- Подсистема обеспечения целостности информации.

Проверка соответствия требованиям по защите информации от НСД АС производится в рамках сертификационных или аттестационных испытаний.

4.1.4 СВТ. Межсетевые экраны. Защита от НСД. Показатель защищенности от НСД к информации.

Документ устанавливает классификацию межсетевых экранов(МЭ) по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Показатели защищенности применяются к МЭ для определения уровня защищенности, который они обеспечивают при межсетевом взаимодействии.

Устанавливаются 5 классов защищенности МЭ, однозначно сопоставленные с классов АС.

`Соответствия класса АС и МЭ.`

Класс МЭ	Класс АС
5	1Д
4	1Г
3	1В
2	1Б
1	1А

Принадлежность тому или иному классу МЭ определяется посредством анализа соответствия показателям защищенности. Ключевая особенность документа состоит в том, что классификация МЭ производится в том числе и по уровням модели ISO/OSI.

4.1.5 Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей.

Документ устанавливает классификацию ПО по уровню контроля отсутствия в нем не декларированных возможностей(НВ). Под НВ понимаются возможности ПО не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Устанавливаются 4 уровня контроля, каждый из которых характеризуется определенной совокупностью минимальных требований. Все требования структурированы.

- требование к документации
- к требование с содержанию испытаний

Испытания проводимые в соответствии с данным документом должны содержать проверки, которые относятся к двум основным категориям: статическому и динамическому анализу.

`Статический анализ исходных текстов программ представляет собой` — совокупность методов контроля соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстовых программ.

`Динамический анализ` — идентификация фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе статического анализа.

Оба метода дополняют друг друга. Результаты статического анализа используются при проведении динамического анализа.

4.2 ГОСТ Р ИСО/МЭК 15408-2002 ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.(Общие критерии)

Одно из преимуществ этого стандарта — его универсальность. Документ состоит `из трех частей`:

1. Введение и общая модель
2. Функциональные требования безопасности
3. Требования доверия к безопасности

В стандарте приведены понятия: Объект оценки(ОО), Продукт, Система.

ОО — понимается произвольный продукт ИТ или система с руководствами администратора и пользователя.

Продукт — совокупность программных, программно-аппаратных или аппаратных средств ИТ, представляющая определенные функциональные возможности и предназначенная для непосредственного использования и включения в состав различных систем.

Система — специфическое воплощения технологий ИТ с конкретным назначением и условиями эксплуатации.

Объект оценки рассматривает с точки зрения среды безопасности(законодательная, административная, процедурная, программно-техническая). При подготовке к оценке анализируется:

1. Предположение безопасности
2. Угрозы безопасности

В стандарт не входит